



UNCLASSIFIED



North Dakota Homeland Security Anti-Terrorism Summary



The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners. If you have any comments to improve this summary or local information you would like to see in the summary please send the information to; kihagel@nd.gov

UNCLASSIFIED

QUICK LINKS

[North Dakota](#)

[Regional](#)

[National](#)

[International](#)

[Banking and Finance Industry](#)

[Chemical and Hazardous
Materials Sector](#)

[Commercial Facilities](#)

[Communications Sector](#)

[Critical Manufacturing](#)

[Defense Industrial Base Sector](#)

[Emergency Services](#)

[Energy](#)

[Food and Agriculture](#)

[Government Sector \(including
Schools and Universities\)](#)

[Information Technology and
Telecommunications](#)

[National Monuments and Icons](#)

[Postal and Shipping](#)

[Public Health](#)

[Transportation](#)

[Water and Dams](#)

[North Dakota Homeland Security
Contacts](#)

NORTH DAKOTA

Fargo to tackle 20 flood projects. Raising the height of Fargo's Fourth Street South levee in North Dakota a couple of feet this summer will cost only about \$125,000, city records show. But done fast enough, the project could save property owners in the Hawthorne and Island Park areas hundreds or even thousands of dollars in flood-insurance payments. The project, one of 20 that city engineers want to tackle this year, would improve flood protection citywide and keep the area out of the 100-year flood plain. However, it must be finished before the Federal Emergency Management Agency decertifies the levee, a senior engineer told city commissioners Friday. The levee, which was once considered 100-year flood protection, is now considered good to a 40-year flood because of vulnerabilities where it ties in to high ground, she said. Commissioners met with staff on Friday to go over an extensive list of projects meant to bring the city's current 37 to 38 feet of flood protection up to the 41- to 44-foot range. The projects would build or improve levees, protect storm sewers, extend drains, raise roads and remove homes along the Red River, Rose Coulee and major county drains.

UNCLASSIFIED

There were some sharp differences on at least two projects. Three projects totaling \$4.2 million, including the Fourth Street levee, are under contract to be done this year. Seventeen other projects totaling \$12.2 million are Priority 1 plans. Those will be the focus of work this summer, though not all are expected to be completed because up to 14 homes must be purchased. Projects needing buyouts will wait until property owners decide they have had enough of flood fighting, officials said. Another four projects worth \$12 million are designated Priority 2. Three of the four projects would require buying 22 homes. Residents will also be encouraged to take part in a backyard, elevation program to cut down on sandbagging until a Red River diversion channel is built to protect the metro area.

Source: <http://www.inforum.com/event/article/id/275772/>

REGIONAL

(Minnesota) Council looks at flooding threats. About \$2 million in work may need to be completed to ensure Winona, Minnesota remains protected against future flooding threats. Winona City Council members Monday approved two studies to assess how much work needs to be done, while using the \$2 million total as a “very rough estimate.” One study will assess whether a drainage ditch carrying water from Lake Winona to the Mississippi River should be dredged. The second will provide an analysis and design to repair or replace four gates at the flood-pump station located at the city’s waste-water treatment plant site. The 2007 flood first alerted city officials to problems with the drainage ditch. Eroded soil carried by Pleasant Valley Creek and deposited in the ditch east of the treatment plant slowed the rate at which water could flow out of Lake Winona. But the city has been unable to gain grant funding or approval for the dredge project because the Minnesota Department of Natural Resources and U.S. Army Corps of Engineers are not convinced the work is necessary, city officials said. The hydraulic analysis by Bonestroo Engineering, which will cost about \$5,800, should provide the data to show the work is needed. The second study will address problems that need to be fixed to keep the Mississippi from flowing up the ditch and into Winona, a path the river water tries to take as water levels rise. The gates cost about \$100,000 to \$120,000 each to be replaced, the mayor said. The analysis would determine if they all need to be replaced and assess any other improvements that might need to be made. Source:

http://www.winonadailynews.com/news/local/article_6a44661c-4c38-11df-ad46-001cc4c03286.html

(Minnesota) Minn. officials warn of eating uneviscerated fish. The Minnesota Department of Agriculture is warning consumers to avoid eating dried fish that still have their internal organs inside. MDA officials found and embargoed more than 400 pounds of so-called uneviscerated fish at ethnic grocery stores in the Twin Cities. The MDA said eating such fish could result in food poisoning. The dried, uneviscerated fish are typically salted and sometimes smoked. Consumers who have any at home are asked to throw it away. There haven’t been any reports of illness linked to consumption of the fish. But MDA officials embargoed the product because of the risk it was contaminated with the bacteria known to produce a potentially deadly toxin. MDA officials are investigating where the product came from and how it ended up in the stores. Source:

<http://www.wday.com/event/article/id/32393/group/homepage/>

(Montana) Roads in Glacier National Park closed due to snow. Officials at Glacier National Park in Montana report that the east side of the park received nearly a foot of new snow this week, sending the plows back to areas already cleared once. It’s a reminder that the progress of the plowing, and subsequent road openings, is completely weather dependent and can change day to day. Most park roads are closed to motorized vehicles due to snow and ice. A few roads are open and they include

UNCLASSIFIED

UNCLASSIFIED

Going-to-the-Sun Road (Sun Road), which is currently open for vehicles 10 miles to Lake McDonald Lodge on the park's west side and six miles to Rising Sun on the east side. The road into Two Medicine Valley is currently open to vehicle traffic to Running Eagle Falls. Kintla Road is open from Polebridge to Big Prairie. Many Glacier Road will be open to vehicle traffic Saturday, April 17. Plowing is complete on the west side of Sun Road from Lake McDonald Lodge to about one mile past The Loop, but parts of the road are covered with ice. Parking remains at the Lodge until the ice melts out. There are usually no restrictions on hikers and bicyclists in effect over the weekend, but that is always subject to change. Starting Monday, April 19, spring construction starts on the west side of the Sun Road, with crews working between Logan Creek Pit and the West Tunnel. Construction, plowing and weather will determine where vehicle and hiker/biker access will be allowed. The Camas Road has been plowed, but a few miles of the road surface are covered with ice. The road remains closed to motor vehicles at this time. Source: <http://www.nps.gov/glac/parknews/news10-20.htm>

(South Dakota) Prescribed burn will take place in Black Hills Forest. In a news release, Black Hills National Forest officials plan to conduct a prescribed burn, Monday, 4 miles southeast of Nemo, South Dakota near the Steamboat Rock Picnic Ground. Objectives of the burn are to reduce hazardous fuels near the wildland urban interface in an effort to create and maintain a forested landscape that inhibits the spread of unwanted fire to crowns of trees. The burn will also provide additional forage for wintering wildlife species. Targeted acres for the burn are 200 to 350 acres depending on appropriate weather and fuel parameters. Smoke will be visible from the I-90 corridor and Rapid City. Resources will be on-site through the night on days when ignition occurs. Source: <http://www.kotaradio.com/news.asp?eid=5002&ID=6143>

NATIONAL

Pacific Northwest in danger of more wildfires. A new study reported by University of Washington (UW) News indicates that, if the Pacific Northwest's temperatures increase by about 3.5 degrees Fahrenheit, the area burned by wildfires each year could double or triple. UW's Climate Impacts Group projects that that type of temperature increase could happen 40 years from now. Some researchers suggest that making forests climate-resistant may include getting rid of surface fuels and thinning more heavily. The research was conducted by UW and the U.S. Department of Agriculture Forest Service. Source: <http://dailyuw.com/2010/4/21/research-insider-maternal-mortality-declining-wild/>

Australian man charged with laundering half-billion dollars in Internet-gambling proceeds. An Australian national was arrested in Las Vegas on April 16 on charges he assisted illegal, Internet-gambling companies by processing approximately \$500 million in transactions between U.S. gamblers and Internet-gambling Web sites and disguising the transactions to the banks so that they would appear unrelated to gambling. In early 2008, the suspect began processing gambling transactions in the United States through the Automated Clearing House (ACH) system which allows money to be electronically transferred from a gambler's U.S. checking account to an Internet-gambling company simply by the gambler going to the Internet gambling company's Web site and entering his bank-account information. The suspect and his co-conspirators processed more than \$543 million in ACH transactions between February 2008 and March 2009, the overwhelming majority of which were on behalf of Internet-gambling companies. The suspect then arranged for the funds received from gamblers to be wired offshore for the benefit of the gambling companies. The suspect also invested

UNCLASSIFIED

UNCLASSIFIED

approximately \$27 million from these ACH transactions into an online “payday loan” company that offered consumers high-interest, short-term loans that typically carried an annualized interest rate of more than 500 percent. The suspect and his co-conspirators induced U.S. banks to provide ACH services to Internet-gambling companies by disguising the transactions so that they would not appear to be gambling related. Source: <http://newyork.fbi.gov/dojpressrel/pressrel10/nyfo041610a.htm>

INTERNATIONAL

Gunmen storm Mexican Holiday Inn, kidnapping at least 6 people. Dozens of gunmen have kidnapped at least six people after storming a Holiday Inn hotel in Monterrey, Mexico’s third-largest city. Police said the heavily-armed gang ran from room to room before abducting a receptionist and four guests. The U.S. consulate in Monterrey has denied media reports that an American woman was among the kidnapped. The Nuevo Leon state attorney general said the violence was probably caused by rivalry between drug gangs in the state following a feud between the Gulf cartel and its former ally the Zetas cartel. Local newspapers said the gunmen hijacked several trucks and used them to block neighboring roads to stop police from chasing them. More than 22,700 people have so far died in drug violence since Mexico’s president launched a military crackdown on organized crime after taking office four years ago. Source: <http://www.foxnews.com/world/2010/04/22/dozens-gunmen-storm-mexican-holiday-inn-kidnapping-people/?test=latestnews>

Govt warns tourists visiting New Delhi. Britain and Australia on Thursday warned tourists of the increased risk of militant attacks in New Delhi, joining Canada and the U.S., which have urged foreigners to avoid parts of the Indian capital. A statement from the British High Commission warned that “there are increased indications that terrorists are planning attacks in New Delhi.” The United States said Wednesday it had information of a “specific” threat to half-a-dozen of the city’s shopping areas and markets which it described as “especially attractive targets.” The Canadian government said on its Web site that an attack could be carried out “in the following days or weeks in market areas” of Delhi frequented by foreigners, specifically in the Chandni Chowk area in Old Delhi. Following this new advice, the Australian High Commission in New Delhi said it “strongly” advised Australians “to minimize their presence in market areas of New Delhi.” The advisories were upgrades to previous, general-advice warning of attacks on prominent business and tourist locations such as Western-owned hotels. In February, a bomb ripped through a crowded restaurant popular with travellers in the western city of Pune, killing 16 people, including five foreigners. It was the first major incident since the 2008 Mumbai attacks in which 10 Islamist gunmen launched an assault on multiple targets in India’s financial capital, killing 166 people. The last major attack in New Delhi was a series of bomb blasts in busy, up-market shopping areas in September 2008 that killed 22 people and wounded 100 more. Source:

http://www.google.com/hostednews/afp/article/ALeqM5i5_bNwKx993lLvP-mu2wYsbreyKA

Iraq’s Northern Oil pipeline explodes; exports halted. An explosion blew a hole in an Iraqi pipeline Thursday, stopping crude oil exports via Turkey, police and oil company officials said. Oil exports should resume within a week, once repairs are completed on the pipeline, an artery through which Iraq pumps one-fourth of its crude shipments, said the head of the production department at the North Oil Co. The explosion was an “act of sabotage,” he said. Unknown saboteurs detonated the explosive charge on the pipeline that runs from Iraq’s Kirkuk oil fields to the Turkish Mediterranean port of Ceyhan, said a police officer. Army and police forces deployed to the scene in al-Hadhar, near

UNCLASSIFIED

UNCLASSIFIED

Mosul, and workers were trying to extinguish the fire, the police officer said. Al-Hadhar is in Nineveh province, where government authorities say insurgents, including extremists from al-Qaeda, frequently carry out attacks. The North Oil Co. currently exports between 450,000 and 650,000 barrels per day, the head of production said. The holder of the world's third-largest oil reserves, Iraq had planned to ship about 16.1 million barrels of Kirkuk oil from Ceyhan in April, according to the state oil company's loading schedule. Source: <http://www.businessweek.com/news/2010-04-22/iraq-oil-pipeline-explodes-north-of-mosul-police-say-update1-.html>

Bomb attacks at Bangalore cricket match raise concerns. A terrorist attack in India has again raised the question of the country's capacity to hold a secure Commonwealth Games. Last weekend, a double, bomb blast outside an International premier league cricket game in Bangalore injured 14 people. Two more bombs were defused outside the stadiums. Indian premier league organizers said security would be tight for the remainder of the tournament. But they have moved the finals, due to begin on Wednesday, from Bangalore to Mumbai. The Australian Commonwealth Games Association said that despite the latest attack, it has faith that the games will be safe. Source: <http://www.radioaustralia.net.au/asiapac/stories/201004/s2877056.htm>

Europe grapples with continuing travel chaos caused by ash cloud. Reeling from disruptions described as worse than those caused by 9/11, European airline and airport operators are appealing for authorities to reassess the flying ban imposed as a result of volcanic ash drifting unpredictably across the continent's skies. As individual governments in the worst-affected countries grappled with the challenges of bringing home citizens stranded abroad – the British government said it would deploy the Royal Navy to retrieve stranded air passengers — the European Union tried to formulate an E.U.-wide response to the crisis. Meanwhile, several airlines took the initiative this past weekend of carrying out their own short, test flights without passengers, attempting a range of altitudes in and around the affected airspace in their regions. No mishaps were reported, and airlines – among them KLM, Lufthansa and British Airways – reported no signs of damage or harm to aircraft systems. Airspace in more than 20 countries has been partly or completely closed, and the ripple effect on long-haul routes has been substantial. U.S. carriers are issuing travel waivers for all flights to, from or through major European hubs until April 22. On Sunday night, the British Met Office reported that the volcano was still erupting and that weather patterns were continuing to blow ash towards the U.K. The International Air Transport Association estimates conservatively that airlines have been losing around \$200 million a day in lost revenue alone, and incurring further significant costs to deal with grounded aircraft and hundreds of thousands of stranded passengers. Source: <http://www.cnsnews.com/news/article/64317>

BANKING AND FINANCE INDUSTRY

Federal Reserve Banks: Areas for Improvement in Information Security Controls. The U.S. Government Accountability Office (GAO) Fiscal Year 2009 audit procedures identified four, new, general information-security control deficiencies related to security management and access controls. It made five recommendations to address these deficiencies. None of the deficiencies identified represented significant risks to the key financial systems maintained and operated by the Federal Reserve Banks (FRB) on behalf of the Bureau of the Public Debt (BPD), the GAO said. The agency found that the potential effect of such control deficiencies on financial reporting relevant to the Schedule of Federal Debt was mitigated by FRB's physical security measures and a program of

UNCLASSIFIED

UNCLASSIFIED

monitoring user and system activity, and BPD's compensating management and reconciliation controls designed to detect potential misstatements in the Schedule of Federal Debt. In addition, during its FY 2009 follow-up on the status of FRB's corrective actions to address 11 open recommendations related to general information security control deficiencies identified in prior years' audits, the GAO determined that as of September 30, 2009, corrective action on eight of the 11 recommendations was completed, while corrective action was in progress on the three remaining open recommendations, which related to security management. The Board of Governors of the Federal Reserve System provided comments on the detailed findings and recommendations in the separately issued Limited Official Use Only report. In those comments, the director of reserve bank operations and payment systems stated that the agency takes control deficiencies, and actions to address them, seriously. The director further commented that three deficiencies have already been addressed or remediated, and that the remainder have corrective actions planned or in progress.

Source: <http://www.gao.gov/products/GAO-10-640R>

Report: 10 percent of fraud victims fall victim to bogus ATM withdrawals. According to a new report released earlier this month by Javelin Strategy & Research on ATM and Personal Identification Number fraud, 10 percent of fraud victims in the U.S. experience fraudulent ATM cash withdrawals. As a result, 23 percent of the 4,874 consumers interviewed for the survey said they left their primary financial institution. Research analysts said that in addition to the use of skimming devices, thieves are now gaining access to customers PINs by manipulating ATM software and by sending out bogus text messages to consumers requesting their personal information. "Despite the efforts by financial institutions to protect consumers, the number of records breached rose 16 percent in 2009," the managing partner and research director for Javelin said in a prepared statement. "Fraudsters have become more organized globally and more sophisticated technologically and may increase their attacks on ATMs in the U.S. as neighboring countries such as Canada and Mexico move to EMV chip-cards, which protect against skimming." Analysts are advising financial firms to not only implement more layered security measures, but to also educate users on fraud risks and how to avoid them.

Source: <http://www.securityinfowatch.com/report-10-percent-fraud-victims-fall-victim-bogus-atm-withdrawals>

Watchdog claims mortgage aid program is vulnerable to scams. Recent changes to the U.S. Presidential administration's mortgage assistance program may make it more vulnerable to fraud, a government watchdog said Tuesday. Announced last month, the changes are intended to make it easier for struggling homeowners to avoid foreclosure. But the administration has not done enough to warn the public about fraud and has not included sufficient safeguards to prevent abuse, the special inspector general for the Troubled Asset Relief Program said in a quarterly report. "Criminals feed on borrower confusion, and frequent changes to the programs provide opportunities for experienced criminal elements to prey on desperate homeowners," the inspector general wrote.

Source: <http://www.businessweek.com/ap/financialnews/D9F6JFP00.htm>

(Michigan) Phone scam results in hundreds of calls to Flagstar Bank. A phone scam involving Flagstar Bank targeted many Jackson-area residents April 19. People reported receiving phone calls with a robotic voice claiming to be from Flagstar and asking for account information. Area police departments and the Jackson County Sheriff's Office were notified of the calls and confirmed with Flagstar that it was a scam. A police sergeant said the sheriff's office received calls all day long. To his knowledge, no one reported giving out sensitive account information. A police sergeant with the

UNCLASSIFIED

UNCLASSIFIED

Parma-Standstone police department said he received two calls about the scam. When he called Flagstar at 7:30 a.m., the bank said it had already received several hundred calls. Source:

http://www.mlive.com/news/jackson/index.ssf/2010/04/scam_results_in_hundreds_of_ph.html

Feds bust website that catered to identity thieves. Federal prosecutors have brought felony charges against an Eastern European man for running a Web site that allegedly helped thousands of criminals exploit stolen financial information. In an indictment unsealed April 19, prosecutors in Manhattan charged the suspect with creating and running CallService.biz. The online business supplied identity thieves with English- and German-speaking individuals to call financial institutions and pose as authorized account holders. They would then confirm fraudulent withdrawals, transfers, and other transactions. CallService.biz, which brazenly advertised its services on other Web sites, assisted more than 2,000 identity thieves carry out more than 5,000 cases of fraud, prosecutors alleged. The Web site was founded in June 2007 and remained in operation until earlier this month. The service was designed to counteract security measures put in place by financial institutions to prevent account fraud. In exchange for a fee, the Web site took online orders that allowed identity thieves to enter instructions about the fraudulent transaction to be conducted over the phone. The Web site would then assign the job to an individual who spoke the appropriate language. Source:

http://www.theregister.co.uk/2010/04/19/identity_theft_website_bust/

(Illinois) Two men indicted in alleged \$56-million bank fraud. Two men who purported to purchase and develop two, Loop residential buildings in Chicago are facing federal fraud charges in connection with financial transactions that allegedly caused the former CIB Bank in west suburban Hillside to lose approximately \$56 million. The defendants allegedly operated various businesses, including a real-estate investment venture, a construction company, a land trust and holding companies. They defaulted on bank loans relating to projects they purportedly undertook at 6 North Michigan Ave., and 59 East Van Buren St. Both men allegedly used at least \$3.6 million in loan proceeds for their own benefit, including to purchase real estate, to buy a vehicle and jewelry for one of the suspects, and to fund the same suspect's investment account. Neither defendant has any connection to the current ownership or development of the two Loop properties. Both suspects were each charged with two counts of bank fraud and three counts of making false statements in bank-loan documents in a federal grand jury indictment that was returned under seal in December 2009. Source:

<http://chicago.fbi.gov/dojpressrel/pressrel10/cg041910.htm>

Regulators close 8 banks. State and federal banking regulators closed eight banks on April 16. TD Bank on April 16 acquired the banking operations of three separate Florida-banking institutions: AmericanFirst Bank, Clermont; First Federal Bank of North Florida, Palatka; and Riverside National Bank of Florida, Fort Pierce. The FDIC estimates that the cost to the Deposit Insurance Fund (DIF) for AmericanFirst Bank will be \$10.5 million; for First Federal Bank of North Florida, \$6 million; and for Riverside National Bank of Florida, \$491.8 million. The FDIC approved the payout of the insured deposits of Lakeside Community Bank, Sterling Heights, Mich. The FDIC estimates the cost of the failure to its DIF Fund to be about \$11.2 million. Butler Bank, Lowell, Mass., was closed; the FDIC entered into a purchase and assumption agreement with People's United Bank, Bridgeport, Conn., to assume all of the deposits of Butler Bank. The FDIC estimates that the cost to the DIF will be \$22.9 million. Innovative Bank, Oakland, Calif., was closed; the FDIC entered into a purchase and assumption agreement with Center Bank, Los Angeles, to assume all of the deposits of Innovative Bank. The FDIC estimates that the cost to the DIF will be \$37.8 million. Tamalpais Bank, San Rafael,

UNCLASSIFIED

UNCLASSIFIED

Calif., was closed; the FDIC entered into a purchase and assumption agreement with Union Bank, National Association, San Francisco, to assume all of the deposits of Tamalpais Bank. The FDIC estimates that the cost to the DIF will be \$81.1 million. City Bank, Lynnwood, Wash., was closed; the FDIC entered into a purchase and assumption agreement with Whidbey Island Bank, Coupeville, Wash., to assume all of the deposits of City Bank. The FDIC estimates that the cost to the DIF will be \$323.4 million. Source: http://www.bankinfosecurity.com/articles.php?art_id=2433

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

Weapons-grade, fissile material in the world could yield 126,500 nuclear bombs. The nations of the world together have in their possession about 1.6 million kilograms of highly enriched uranium (HEU) and about 500,000 kilograms of plutonium. Because it takes only about 25 kilograms of HEU or eight kilograms of plutonium to make a crude, nuclear bomb, the weapon-grade material now available in the world could yield 64,000 HEU-based bombs and 62,500 plutonium-based bombs. This information came out during the nuclear summit hosted by the U.S. President convened in Washington, D.C. from April 12 to 16. The convention focused less on nuclear weapons and more on more poorly guarded nuclear materials that could be used to build weapons or dirty bombs. The reason for this focus: Obtaining enough plutonium or highly enriched uranium is the most important step toward getting a nuclear weapon. A former U.S. ambassador-at-large for nonproliferation issues said it is possible that al Qaeda or some other terrorist group could steal or buy ready-made nukes. The world's warheads, however, are relatively secure and accounted for. The stockpiles of fissile materials sprinkled around the globe are another matter. "I think the chances of Al Qaeda acquiring fissile material and making its own improvised nuclear device are greater than the chances it will get an already-fabricated weapon and detonate that," said the ambassador, now president of the MacArthur Foundation, in a Monday speech. Fissile material is held at hundreds of locations, with varying levels of security. There are more than 130 research reactors alone that are powered by HEU, some of them in developing or transitional countries, notes the Belfer Center. Source:

<http://homelandsecuritynewswire.com/weapon-grade-fissile-material-world-could-yield-126500-nuclear-bombs>

COMMERCIAL FACILITIES

(Texas) Wichita Falls gunman who killed 1, wounded 4 yelled 'white power,' witness says. A 22-year-old man with a violent history shot up a crowded, bookstore cafe, wounding four women, then walked down the street and killed a bar worker before holing up in a home where he killed himself, authorities said Wednesday. The man rampage may have been motivated by racial hatred, a police sergeant said. "A recurring theme from witness statements was that the suspect was yelling racial epithets," he said. A witness told the Wichita Falls Times Record News that the gunman shouted "White power!" before fatally shooting a 23-year-old bar doorman. Witnesses said the incident began late Tuesday when the suspect walked into a bookstore cafe and started firing a shotgun, wounding four women. Although both the shooter and the doorman were white, three of the wounded women are black and the other is Hispanic, the police sergeant said. None of the women suffered life-threatening injuries, though three remained hospitalized Wednesday at Parkland Memorial Hospital in Dallas. Court records show the gunman was facing aggravated assault charges in the October 19 stabbing of two men at a Lake Wichita park and had been sentenced to probation in 2008 after pleading guilty to aggravated robbery. He also was charged with aggravated assault on December 31

UNCLASSIFIED

UNCLASSIFIED

for allegedly hitting and threatening to kill a girlfriend. The Air Force and FBI are assisting in the investigation because two of the wounded women were temporarily stationed at nearby Sheppard Air Force Base, a base spokesman said. They were listed in stable condition Wednesday, he said. The condition of the third woman transported to Parkland was not available. The fourth victim was released from a Wichita Falls hospital, the police sergeant said. Source:

http://www.dallasnews.com/sharedcontent/dws/news/texasouthwest/stories/DN-shooting_22tex.ART.State.Edition1.4cb6bca.html

(Illinois) Bomb squad responds after police find explosives in Chicago apartment. A 36-year-old Chicago man is facing charges after police say they found explosives at his apartment and called the bomb squad. A man was charged with felony possession of an explosive or incendiary device and misdemeanor, domestic battery after the incident Sunday. Police said they were called to his apartment on Chicago's near West Side for a domestic incident. According to a police report, authorities found 12 "improvised explosive devices" at the home. The report said the explosives were "rendered safe" by two police bomb-squad technicians. Source: <http://www.wqad.com/news/sns-ap-il--chicago-explosivesfound,0,290140.story>

(Virginia) Bomb scare at Sugarland shopping center. Emergency crews spent much of the day Friday dealing with a suspicious package in the parking lot of the Sugarland Run Crossing shopping center in Sterling, Virginia. The package was deemed harmless by the county bomb squad. Loudoun County deputies were called to the scene around 2:45 p.m. A portion of the shopping center was closed as a precaution while authorities addressed the situation. The incident cleared around 7 p.m. Source: <http://www.google.com/reader/view/?hl=en&tab=wy#stream/user/14538411749081893480/label/Commercial>

COMMUNICATIONS SECTOR

Undersea telcoms cables face growing risks-report. Investors should urgently diversify the web of undersea cables that serve as the world's information and banking arteries to address soaring demand and piracy concerns and reduce the risk of catastrophic outages. So says a report by a multinational research project that calls for the building of global backup routes for the submarine network that carries almost all international communications, including financial transactions and Internet traffic. The report's main author of the Institute of Electrical and Electronics Engineers (IEEE), an international professional body, told Reuters changes should be made "before we have to learn the hard way." "This report is trying to have a September 10 mindset, where you actually do something about what you know on September 10 to avoid a September 11 situation," the main author who was an adviser to the U.S. government on cybersecurity after the September 11 attacks said. An executive summary of the report made available to Reuters says that the current probability of a global or regional failure of the network is very low, but is "not zero". "The impact of such a failure on international security and economic stability could be devastating...There is no sufficient alternative back-up in the case of catastrophic loss of regional or global connectivity." Source: <http://www.reuters.com/article/idUSLDE63J0NJ20100420?type=marketsNews>

Satellite system won't see space anytime soon. Delays plaguing the Navy's Mobile User Objective Satellite program have yet to end, with one DOD official confirming the initial launch has been pushed back yet again to late 2011. "Hopefully, in the next two years we will be able to replace the

UNCLASSIFIED

UNCLASSIFIED

[current ultra-high frequency satellite] constellation,” a Navy captain and deputy commander, Space Field Activity, Space and Naval Systems Command, said April 15 at the AFCEA Naval IT Day in Vienna, Virginia. “We’re focusing on launching in late ‘11, with on-orbit capability in 2012.” With MUOS years behind schedule, the Navy is looking to the commercial sector to bridge the gap between the expiration of the current ultra-high frequency follow-on satellites and the yet-to-be-launched MUOS satellites. Naval officials are also asking Congress to consider yielding some government-only UHF bandwidth to commercial operators to help ease the transition. The existing satellites provide critical capabilities for all four military branches, including communications, navigation and geo-location used for precision weapons. But they are aging and obsolete, and narrow-band capabilities will degrade below the required level of availability by January 2011 if no interim measures are taken, according to the Government Accountability Office. The degraded, narrow-band communications could result in outages on the ground that would slice into the operations of soldiers, sailors, Marine and airmen around the world. Source: <http://defensesystems.com/articles/2010/04/19/muos-update-more-delays.aspx?admgarea=DS>

DEFENSE INDUSTRIAL BASE SECTOR

Gates points out dangerous gaps in US defense exports. In the fight to keep sensitive, government technologies and equipment out of the wrong hands, the administration plans a radical overhaul of a Cold War-era system more alert to the likes of Soviet spies than modern terrorists. The Secretary of Defense, discussing a review ordered by the President last summer, said the current Defense Department and Commerce Department systems for licensing the export of such technologies are so deeply flawed, in fact, that they pose a national security threat. The secretary spoke a month after a Government Accountability Office investigation found that a wide range of U.S. military and dual-use goods, including military aircraft parts, had been illegally shipped to Iran despite U.S. sanctions. The current system is based on “two different control lists administered by two different departments, three different primary licensing agencies, [and] a multitude of enforcement agencies with overlapping and duplicative authorities,” the White House added in a statement outlining the president’s proposed fixes. Moreover, it said the agencies involved are using a tangle of conflicting information technology systems — or no IT system at all. The secretary said that diffusion of authority means that those who are refused an export license by one agency can try their luck with another. At the same time, the system makes it hard for U.S. allies to get urgently needed parts in a timely manner, such as nuts and bolts for a plane whose export has already been approved. To deal with the problem, the administration wants “to build high walls around a smaller yard,” the White House said. The new system would feature a single export-control list shared by all participating offices at the Defense, Commerce, State and Treasury departments. It would create a single, unified export-licensing agency, a single enforcement agency and one, unified IT system to track it all. Source: <http://www.aolnews.com/nation/article/defense-secretary-gates-calls-out-dangerous-gaps-in-us-military-exports/19447744>

Stratcom rings missile-warning-gap alarm. Concerns are once again surfacing at U.S. Strategic Command about a potential gap in the critical mission area of space-based missile warning. Last December the Stratcom commander issued an urgent-need request to the Operationally Responsive Space (ORS) office for alternatives to augment the mission, according to a Stratcom official. At issue is the timing of a transition between the Defense Support Program (DSP) constellation and the new Space-Based Infrared System (SBIRS) constellation being manufactured by Lockheed Martin Space

UNCLASSIFIED

UNCLASSIFIED

Systems. Delivery of SBIRS GEO-1, which will be the first spacecraft bound for geosynchronous orbit to replace DSP, is at least seven years late. And the program, now estimated at \$15 billion, is costing far more than expected. DSP, and eventually SBIRS, will provide the early cue for defenses in the event of a ballistic missile attack against the U.S. or points abroad. However, the availability of GEO-1 is not part of the coverage gap worries. The Air Force Space Command chief said the satellite would likely be launched in early 2011 and officials are exploring ways to extend the life of the DSP constellation. The second SBIRS satellite is slated to be lofted roughly a year after GEO-1. But there was a gap in purchasing the third satellite and beyond, and this could potentially lead to holes in coverage. Source:

http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/awst/2010/04/19/AW_04_19_2010_p35-219773.xml

(Tennessee) Y-12 plays a role in securing uranium. Amid ultra-tight security, just days before the February 27 earthquake rocked Chile, three employees from the Y-12 nuclear weapons plant were taking care of business at a research reactor 20 miles from the capital city of Santiago. They were carefully packaging highly enriched uranium fuel - material that could be converted into a nuclear weapon - for eventual transport to the Oak Ridge nuclear plant in Tennessee for safe-keeping. The secret mission, carried out with the cooperation of Chilean authorities, was similar to dozens of other projects conducted around the world in recent years to keep terrorists from getting their hands on nuclear materials. Y-12 played a role in some of those recovery projects, and that role could grow as a result of last week's Nuclear Security Summit in Washington, D.C., where representatives of 47 nations pledged to secure all vulnerable nuclear material within four years. Historically, the Oak Ridge plant has produced uranium parts for every nuclear weapon in the U.S. arsenal, and it is that uranium expertise that has made Y-12 a valuable player in nonproliferation and counter-terrorism efforts.

Source: <http://www.knoxnews.com/news/2010/apr/18/y-12-plays-a-role-in-securing-uranium/>

CRITICAL MANUFACTURING

Toyota recalls 2010 Lexus SUVs. Toyota has announced the recall of 9,400, luxury SUVs less than a week after Consumer Reports highlighted what it called a "dangerous flaw" in the vehicle. Toyota, Monday, said it would recall the 2010 Lexus GX 460 models sold in the United States to address an electronic, throttle issue. "With the news from Consumer Reports that our 2010 GX 460 did not pass its "Throttle Lift-Off" test, we immediately stopped selling the vehicle and commenced vigorous testing to identify and correct the issue," Toyota said in a statement. "Today, I'm happy to announce that we have developed a remedy that will be quickly implemented to address customer concerns," said the Lexus Group vice president and general manager. "We will be voluntarily recalling all 2010 GX 460s that have been sold in order to update the vehicle stability control system. We will begin implementing this program in the next two weeks and our dealers will be reaching out to customers shortly to set up appointments to make this modification." Lexus said it is confident that the update would improve GX performance. The company also said it would provide a courtesy vehicle to anyone who has purchased a 2010 GX 460 and has concerns about driving it until the recall work has been completed. Source: http://www.consumeraffairs.com/news04/2010/04/lexus_recall.html

Toyota to recall 600,000 minivans. Toyota Motor Corporation said Friday it was recalling 600,000 Sienna minivans sold in the United States to address potential rusting, spare-tire cables that could break and create a road hazard in the latest safety problem to strike the beleaguered automaker. The

UNCLASSIFIED

UNCLASSIFIED

recall came as U.S. House of Representatives' investigators said they planned to hold another congressional hearing in May to review potential electronic problems in runaway Toyotas. The Japanese automaker has recalled more than 8 million vehicles because of faulty accelerator pedals, humbling a car company long known for its quality and safety. Separately, Toyota said Friday its engineers in Japan had duplicated the same results of tests that led Consumer Reports to issue a rare "don't buy" warning on the 2010 Lexus GX 460 over rollover concerns. Toyota responded by halting sales of new GX 460s and conducting tests on all of its SUVs. Toyota said its latest recall covered the 1998-2010 model year Siennas with two-wheel-drive that have been sold or registered in 20 cold-climate states and the District of Columbia. Toyota said rust from road salt could cause the carrier cable that holds the spare tire to rust and break, allowing the tire to tumble into the road. The problem could threaten the safety of other drivers. Source:

http://www.nytimes.com/aponline/2010/04/16/us/AP-US-Toyota-Recall.html?_r=1&partner=rss&emc=rss

EMERGENCY SERVICES

(California) California to track 911 calls statewide through centralized system. There is no official standard for equipment configurations or the technology that call centers use for data gathering. And that makes it tricky to compare emergency call statistics — especially in big states such as California, which has nearly 500 public-safety answering points (PSAPs) and had been using two, separate systems, from AT&T and Verizon. "The interfaces and everything were different," said the acting chief of the state's 911 office. "It made it difficult to pull data and compare it." Now California is deploying a solution that could cut the time it takes to gather the state's 911 call data from months to a matter of minutes. It's called the Emergency Call Tracking System. This secure, Web-based management tool can report on all 911 PSAPs in an entire county, jurisdiction or state, giving clients quick access to key stats such as call volume, frequency, type, and geographical trends Source:

<http://www.govtech.com/gt/articles/754469>

Defense to use systems to share threat information. The U.S. Defense Secretary announced Thursday that he has directed the Defense Department to use a law-enforcement database sometimes referred to as Google for cops to identify military personnel who could pose a threat. The goal is to prevent violent incidents such as the Fort-Hood, Texas shootings. An independent, review panel assembled after an Army major killed 13 people at the Army base on Nov. 5, 2009, submitted a report to the defense secretary in January, in which it made 79 recommendations to improve safety. The study described a systemic gap in sharing of data about potential, insider threats, and in exchanging information with state and local-law enforcement agencies. The problem could be solved by using Navy and FBI systems, the report said. Intelligence agencies had gathered information on the Fort-Hood suspect months before the attack that revealed he had been in contact with al Qaeda terrorists. However, the evidence did not reach Army or Fort Hood commanders. LInX will be renamed the Law Enforcement National Data Exchange, and the Defense Secretary asked the undersecretary of Defense for personnel and readiness to deploy it in 2011. Source:

http://www.nextgov.com/nextgov/ng_20100416_3573.php

Emergency network still needed, FCC public safety chief says. Despite public pressure to keep federal spending in check, the Federal Communications Commission's top, public-safety official renewed his call for creation of a \$16-billion, national data network for public safety workers to be

UNCLASSIFIED

UNCLASSIFIED

partly financed by a monthly fee on all broadband users. “I’d say to the average citizen who wonders why this is needed, ‘Do you want your mom’s police department to be able to interoperate with the sheriff’s department and the national guard in a crisis?’ ” said the chief of the FCC’s public safety and homeland security bureau. “Most will say yes. For a few cents a month, we will make sure we have that ability.” He suggested the public safety fee could be as low as 50 cents a month on every broadband user, although the FCC’s National Broadband Plan announced in March calls for a “minimal” fee without listing an amount. Source:

http://www.computerworld.com/s/article/9175686/Emergency_network_still_needed_FCC_public_safety_chief_says

ENERGY

(Colorado) Xcel to shut or convert Colorado, coal power plants. Xcel Energy, the largest utility in Colorado, will retire, retrofit or repower about 900 megawatts of coal-fired generation to reduce air pollution under a new law signed by the governor this week. Units at three Denver-area coal plants are being evaluated for possible retirement or conversion to burn natural gas, an Xcel spokesman said. The sites being studied include a 186-megawatt coal unit at the Valmont plant, four units, totaling 717 MW, at the Cherokee station and a 505-MW coal unit at the Pawnee station. Under the Clean Air-Clean Jobs Act, Xcel will submit a plan to state regulators in August to reduce its nitrogen-oxide (NOX) emissions from coal units by up to 80 percent from 2008 levels by 2017. The plan will likely include a combination of unit retirement, replacement with gas turbines or installation of improved pollution-control equipment, the spokesman said. Reducing NOX emissions at power plants and other industrial sites will help Colorado as it works to comply with federal clean-air standards.

Source: <http://www.reuters.com/article/idUSN2010698620100420>

Katrina led to onshore petroleum releases. A National Science Foundation-funded study suggests Hurricane Katrina caused more than 200 onshore releases of hazardous materials along the Gulf Coast. The researchers said they used data from the U.S. Coast Guard’s National Response Center Incident Reporting Information System. They said they found about 8 million gallons of petroleum releases were reported as a result of Katrina hitting the U.S. Gulf Coast in 2005 — mostly due to storage tank failure and the restart of production processes. The scientists said many refineries and other facilities shut down in anticipation of large storms to minimize damage. However, shutdowns and their subsequent restarts can lead to large emissions of volatile organic compounds and other chemicals. “More attention should be given to planning for shutdowns, including coordination with government entities responsible for evacuation, and to plant startup after an emergency shutdown in order to minimize burning off excess gas by flaring and other releases,” the researchers said. The study is reported in the journal Risk Analysis. Source:

http://www.upi.com/Science_News/2010/04/19/Katrina-led-to-onshore-petroleum-releases/UPI-35751271709218/

(Massachusetts) Thousands without power after problem at National Grid substation. Thousands of people in Lynn, Saugus and Swampscott, Massachusetts, found themselves without power Monday morning, following a substation problem with National Grid. A spokeswoman said most customers were restored as of 11 a.m., but said roughly 4,000 remained without power until 11:45 a.m. “It appears to have been a faulty piece of equipment at the substation in Lynn that caused the outage,”

UNCLASSIFIED

UNCLASSIFIED

she said. "It's always our priority to get our customers back in service and the engineers continue to look into the problem." Customers were able to be quickly restored through a process she called "switching," which feeds customers on other lines. Source:

<http://www.thedailyitemoflynn.com/articles/2010/04/20/news/news07.txt>

FOOD AND AGRICULTURE

Fecal bacteria contamination widespread in bagged salads. A recent Consumer Reports investigation has revealed that bagged salads labeled "pre-washed" or "triple-washed" may not be as clean as they appear. Of the 208 samples taken from 16 different brands of bagged salad, researchers found that nearly 40 percent of them were tainted with bacteria often found in fecal material. The tainted salads were not contaminated with more serious bacteria like salmonella or E. coli, but 39 percent of them did contain coliform levels that exceeded 10,000 colony forming units per gram (CFU/g) and 23 percent of them contained enterococcus levels exceeding 10,000 CFU/g. Industry experts generally agree that acceptable levels of these types of bacteria for leafy greens should be below 10,000 CFU/g. Coliform bacteria does not necessarily come from feces, but high levels of the types found in some bagged salads does suggest that poor sanitation practices likely caused fecal contamination. The U.S. Department of Agriculture (USDA) has also admitted that trace amounts of salmonella can be found in about two out of every 4,000 bags of salad. Source:

http://www.naturalnews.com/028628_salad_feces.html

Contaminated dips recalled. East Coasters who bought spinach or artichoke dip recently, should check the label. Giant Food and Stop & Shop Supermarkets have announced a voluntary recall of frozen artichoke and spinach dips that may be contaminated with *Listeria monocytogenes*. Although healthy people rarely get sick from the bacteria, *Listeria monocytogenes* can cause listeriosis, a serious infection that poses significant risk for babies, the elderly, and pregnant women. *Listeria* is usually killed by pasteurization and cooking; it's unclear why the bacteria may be present in the affected dips. Customers who purchased the dips are advised to throw it away and bring in their receipts for refunds. Giant Foods said it hasn't gotten any reports of illness thus far. The supermarkets in question are mainly located along the Eastern seaboard. Giant Foods is based in Landover, Maryland with locations in Maryland, Virginia, Delaware and the District of Columbia. Stop & Shop's home base is in Quincy, Mass. and has stores in Massachusetts, Connecticut, Rhode Island, New Hampshire, New York and New Jersey. The Stop & Shop frozen dip being recalled is in an eight-ounce container with the UPC code: 6 8826702988 2. The Giant Food dip being recalled is in an eight-ounce container and has the UPC code: 6 8826702988 2. Source:

<http://www.slashfood.com/2010/04/19/contaminated-dips-recalled-stop-and-shop-giant-food-supermarkets/>

(Kansas; Louisiana; Texas) Fungus found in Texas, Louisiana wheat; may threaten Kansas. A yield-reducing fungus is attacking winter wheat fields across parts of the South, and plant disease specialists are concerned it could soon spread north to Kansas, the nation's top-producing wheat state. The disease, called stripe rust, is caused by the fungus *Puccinia striiformis* and often causes yield losses of around 40% on susceptible wheat varieties. It can destroy fields outright if not treated quickly with chemical fungicides. The pathogen – which is spread by the wind and thrives in cool, damp weather such as what has predominated this spring – has been found in wheat throughout Louisiana and has even infected popular varieties thought to be resistant. Several cases of severe leaf

UNCLASSIFIED

UNCLASSIFIED

rust and stripe rust were found in multiple locations around Texas during March, occurring in some hard red winter (HRW) wheat varieties previously thought to be highly resistant to the disease, such as Fuller, Santa Fe, Art, Overley, Jagger and Jagalene. “The severity of the disease on varieties previously thought to be resistant is cause for concern,” said a Kansas State University plant pathologist. “I believe these reports of stripe rust and leaf rust have important implications for wheat producers in Kansas. Fuller, Santa Fe and Art are all widely grown in central Kansas.” While no stripe rust has been yet reported in neighboring Oklahoma or Arkansas, stripe rust is likely lurking, said a plant pathologist with the University of Arkansas Division of Agriculture. Wheat-disease specialists are now working to determine if the outbreak is evidence of an underlying genetic mutation in the stripe rust fungus, which was once confined solely to the Pacific Northwest. Source:

<http://cornandsoybeandigest.com/eWheat/wheat-fungus-found-0420/>

ABC grills Vilsack on meat residues. In response to the recent U.S. Department of Agriculture (USDA) Office of the Inspector General (OIG) report, which found that the agencies responsible for monitoring veterinary drug, heavy metal, and pesticide residues are “not accomplishing” their mission, an ABC Television news anchor sat down the the U.S. Agriculture Secretary to discuss the findings. “Can the public be assured that beef with potentially dangerous substances is not on the market?,” the news anchor asked. “I think that they can because of the focus the President has placed on food safety,” replied the Agriculture Secretary, noting the creation of the President’s Food Safety Working Group (FSWG). “Are inspectors catching all of the beef that may contain potentially dangerous substances, now?” the anchor asked. The Agriculture Secretary said that inspectors are “in the process of improving what they do ... I think we can assure people that we have a safe and ample supply of food in this country. What people must understand and appreciate is that we are taking this report very seriously and we’re following up on the recommendations.” But the Agriculture Secretary noted that the USDA’s Food Safety and Inspection Service does not have the authority to mandate a recall of meat found to have excessive levels of antibiotics, heavy metals, or pesticides. “We can ask the supplier to recall, but statutorily we do not have the power,” he explained. “The power we have is for us to remove our inspectors from a plant, which effectively shuts down the plant. In terms of mandatory recall authority, we don’t have that.” Source:

<http://www.foodsafetynews.com/2010/04/abc-grills-vilsack-on-meat-residues/>

(Ohio) Crops threatened by large volume of honeybee deaths. An estimated 50 to 70 percent of hives kept by Ohio beekeepers died over the winter, said a spokeswoman for the Ohio Department of Agriculture. The losses are in keeping with heavy fatality rates experienced since 2006 — a year when 600,000 bee colonies in the U.S. mysteriously fled their homes and disappeared, said Ohio’s state honeybee specialist. “The average person should care,” he said. “Bees of all species are fundamental to the operation of our ecosystem.” Without bees to pollinate vegetables like squash and fruits like pears, apples and blueberries — a third of the human diet — you’d be looking at a menu of wheat and corn,” the honeybee expert said. Bees annually pollinate Ohio crops worth \$44 million, including berries, fruits and vegetables. Honeybees are under siege from many foes: Destructive mites, pesticides, a mysterious disorder that causes them to abandon hives, and stress from overwork to pollinate cash crops. In the 1920s, Ohio beekeepers kept 120,000 colonies. Today, there are about 30,000. Source: <http://www.daytondailynews.com/news/dayton-news/-44m-in-crops-threatened-by-high-honeybee-deaths-through-winter-660027.html>

UNCLASSIFIED

UNCLASSIFIED

(California) Undeclared wheat brings meat recall. By mistakenly not disclosing wheat starch on the ingredient label, a California meat processor has been forced to recall 140,000 pounds of fully cooked assorted products. Santa Ana, California-based Westlake Food Corporation issued the recall over the weekend, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) said. Wheat is a known allergen. FSIS said there is low health risk involved in the Class II recall, except for people with wheat allergies. The products subject to recall include: 14-ounce packages of Gio Lua Tay Ho Pork Meat Loaf Wrapped in Banana leaves fully cooked; 13-ounce packages of Bo Ven Tay Ho Beef Meat Ball Fully Cooked; 14-ounce packages of Doi Gio Heo Tay Ho Cured Pork Hock Sausage With Onion Wrapped in Pork Skin Fully Cooked; 15-ounce packages of Cha Chieen Tay Ho Fried Pork Pattie Fried in Vegetable Oil Fully Cooked; 13-ounce packages of Bo Vien Gan Tay Ho Beef Meat Ball With Beef Tendon Fully Cooked that was produced between April 15, 2009 and April 14, 2010. Each package bears the establishment number "EST. 1627A" inside the USDA mark of inspection. The products were produced between January 1, 2010 and April 14, 2010, unless otherwise noted above. These products were distributed to restaurants and retail establishments nationwide. The labeling error was discovered by FSIS during a routine inspection. FSIS and the company have received no reports of adverse reactions due to consumption of these products. Source:

<http://www.foodsafetynews.com/2010/04/undeclared-wheat-brings-meat-recall/>

School food safety inspections lacking. Although federal law requires schools across the country to have food safety inspections twice a year, nearly 9,000 schools during the 2007-2008 school year did not. According to data from the U.S. Department of Agriculture's Food and Nutrition Service (USDAFNS), almost 27,000 schools received one food safety inspection or were not inspected at all. Certain health standards are required by every school that serves meals as a part of the federally funded National School Lunch Program or the School Breakfast Program. According to a USDAFNS spokeswoman, "They are checking for cleanliness, hazard procedures, and if the food is at the appropriate temperature. Not doing them [the inspections] is not meeting the requirements set forth by law." About 70,000 schools in the U.S. met or exceeded two inspections during the 2007-2008 school year according to the latest reports. Ranked highest, with 98 percent having met the requirement, was Tennessee. Maine ranked the worst, having reported 98 percent of schools had received one inspection or less. "We know across the country that local and state governments are being squeezed, and they may not have enough inspectors to get to every place," the USDAFNS spokeswoman said. "While we are sensitive to the concerns and challenges to getting these done, they do need to be completed." Source: <http://www.foodsafetynews.com/2010/04/school-food-safety-inspections-lacking/>

Tracing Listeria monocytogenes in a commercial chicken cooking plant. Incoming raw poultry is the primary source of Listeria monocytogenes contamination in commercial, chicken-cooking plants, according to a 21-month study conducted by Agricultural Research Service (ARS) scientists and their University of Georgia collaborators. The goal is to help such facilities focus sanitation processes to reduce cross-contamination. L. monocytogenes is a bacterial human pathogen that is sometimes found in fully cooked, ready-to-eat processed meat and poultry products. By testing a brand-new, commercial cooking facility before and after processing began, the research team was able to track many sources of contamination, including employees, incoming fresh air, raw meat, and the surrounding environment. Researchers tested soil and water samples near the facility exterior, tested incoming air from air vents, and tested heavily traveled floor surfaces following personnel shift changes. They also took monthly swabs of incoming raw meat. The plant was free of L.

UNCLASSIFIED

UNCLASSIFIED

monocytogenes when first constructed; floor drains were sampled monthly to determine when the plant would become colonized. Within four months of operation, *L. monocytogenes* was detected in floor drains, indicating the organism had been introduced from an outside source. No bacteria were recovered from any floor samples in the plant entryways, locker room or cafeteria. Likewise, the organism was not detected on air vent filters during the survey. The only tested source found to be consistently positive for *L. monocytogenes* was incoming raw poultry meat. This research was reported in the Journal of Food Protection. Source: <http://www.ars.usda.gov/is/pr/2010/100419.htm>

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(Massachusetts) Wareham students charged with making bomb threats. A Wareham, Massachusetts police school resource officer and a Wareham fire department investigator have been investigating false bomb threats at two Wareham elementary schools. A bomb threat was written on a bathroom wall at the Minot Forest School on March 25. Police investigators learned of a bomb threat April 14, posted on a social networking Web site that targeted the John Decas Elementary School. Wareham fire and police investigations determined that both threats were false. Further investigation by the school resource officer and Wareham police identified two juvenile students, one at each school, who were responsible for the pranks. The students have been charged with making false bomb threats and will face a juvenile clerk magistrate's hearing in Wareham District Court at a future date. Last week, police arrested an 18-year-old Wareham man in connection with an April 13 bomb threat at Wareham High School. Source: <http://www.enterpriseneews.com/news/x1042542495/Wareham-students-charged-with-making-bomb-threats>

Greece: Evidence found on US embassy attack. Evidence links suspected members of a domestic terrorist group to a 2007 rocket-propelled grenade attack on the U.S. embassy in Athens, Greek police said Thursday. The police chief said computer hard drives found in a backpack left inside a car owned by one of the six arrested suspects contained statements and drafts by Revolutionary Struggle, including one claiming responsibility for the embassy attack. The attack damaged the front of the embassy building. Two handguns, ammunition, and euro119,240 (\$161,500) in cash were also found in the backpack. The six suspected members of the far-left militant group were arrested over the weekend, during multiple raids. The suspects - five men and one woman aged between 30 and 41 - have been charged with multiple counts of attempted homicide, causing explosions, and arms-possession offenses. They face up to 25 years in prison if found guilty on the main charges. The police chief said the hard drives were found in the backpack in the truck of the car, which also contained the guns and money, along with three, fake state-identity cards, all bearing the same photograph of one of the suspects. "The two handguns have not been used in any criminal activity," the police chief said. The discovery announced Thursday follows daily raids on suspected safe houses used by the group. Authorities are still searching for the group's main arms cache. Source: <http://www.lasvegassun.com/news/2010/apr/18/greece-evidence-found-on-us-embassy-attack/>

(California) Neo-Nazi rally becomes standoff. A neo-Nazi white supremacist group rallied against illegal immigration in downtown Los Angeles on Saturday as hundreds of counter-protesters gathered to shout them down in a tense stand off that included thrown rocks and police in riot gear. Police officers stood between the white supremacists and counter-demonstrators on the south lawn of Los

UNCLASSIFIED

UNCLASSIFIED

Angeles' City Hall, where about 50 members of the National Socialist Movement waved American flags and swastika banners for about an hour. There was a brief flare-up of violence when a man removed his shirt revealing tattoos that featured Nazi lightning bolts. Two men were treated at a hospital for minor injuries and released, police said. As the rally ended, counter-protesters hurled rocks, branches, and other items over the police line toward the neo-Nazis. Police said a few counter-protesters were arrested for throwing items. Source:

<http://www.heraldnet.com/article/20100418/NEWS02/704189880>

Shortcomings in U.S. safeguards of weapon-grade nuclear materials. Reviews ordered by the U.S. President have found weaknesses in the U.S. government's stewardship of its nuclear cache, from weapons to the ingredients and classified information that go into them. Several recent reviews have found weaknesses in the government's stewardship of its nuclear cache, from weapons to the ingredients and classified information that go into them. The following are among the findings. The Air Force in January removed an entire squadron overseeing a bunker of nuclear warheads at Kirtland Air Force Base in Albuquerque, New Mexico, citing a failed inspection that it blamed on administrative problems. In March, the Government Accountability Office detailed problems with a program under which at least thirty-four metric tons of weapons-grade plutonium is to be disposed of in fuel for nuclear power plants. The Energy Department inspector general reported in January that the Sandia National Laboratories in New Mexico had not removed some highly enriched uranium while carrying out a department plan to consolidate nuclear materials into the most secure environments possible. Last fall, the GAO reported that the Los Alamos National Laboratory, another nuclear weapons lab in New Mexico, had several security lapses in protecting classified information on its computers. In September, the congressional investigators recommended that the Pentagon make several improvements in its process for assessing threats to installations where nuclear weapons are stored, maintained, or transported. Source:

<http://homelandsecuritynewswire.com/shortcomings-us-safeguards-weapon-grade-nuclear-materials>

Pentagon to revise gun rules for military bases. The Pentagon will adopt a broad policy governing how privately owned guns can be carried or stored at military installations after the shooting deaths of 13 people last year at Fort Hood, Texas. The Army psychiatrist charged in the killings had little or no access to military firearms in his job but was able to buy two handguns and bring them onto the base. A Pentagon investigation into the killings concluded that the policy on carrying personal weapons on military bases was inadequate and that communication between the FBI and military was inconsistent. In response, the Pentagon on Thursday released a summary of actions, including the weapons-policy change, ordered by the Department of Defense Secretary for security and administrative upgrades. The secretary ordered that the new, comprehensive weapons policy be developed to cover all branches of the military and its bases and offices. The new policy is expected to mirror restrictions already in place at some military installations that, for example, require guns brought onto a base to be registered with military police. Source:

http://www.dallasnews.com/sharedcontent/dws/news/nation/stories/DN-forthood_16nat.ART.State.Edition1.4c70b85.html

(Tennessee) Man threatens to blow up government office. A Coffee County (Tennessee) man was arrested Friday for allegedly making threats to commit a terrorist act. The sheriff's department said the suspect called the register of deeds on Thursday and threatened to shoot workers and their

UNCLASSIFIED

UNCLASSIFIED

families, as well as blow up the office. The suspect, 66, works for the official, and it is not the first time he's made such threats, the sheriff said. Currently undergoing psychological evaluation, the man is being held on a \$100,000 bond. Source: <http://www.wsmv.com/news/23175292/detail.html>

Analysis: College leaders should review threat-assessment capacities. Colleges and universities should review their threat-assessment capacities because some of the conventional beliefs about these attacks are not accurate, a new report issued by the federal government shows. For example, while much attention is given to the "traveling" attacker, such as the student who killed 32 students in a shooting spree at Virginia Tech on April 16, 2007, only 3 percent of perpetrators of campus violence actually moved from building to building. Ever since 23-year-old shooter, killed 32 students and wounded 17 at Virginia Tech, college leaders have been reviewing and improving their threat-assessment procedures and their ability to respond to a dangerous situation. They must reassess their approach, according to the new report, called "Campus Attacks: Targeted Violence Affecting Institutions Of Higher Education," which was just issued jointly by the U.S. Secret Service, the Education Department and the Federal Bureau of Investigation. The study analyzed 272 acts of violence against specific targets on college campuses in 42 states and Washington D.C., from 1900 through 2008. The attacks resulted in 281 deaths, including 190 students and 72 employees. Another 247 people were injured in attacks on campuses, including 144 students and 35 employees. Most of the attacks were carried out by one person. About 94 percent of the perpetrators were male, and they had an average age of 28, the report said. Source: <http://voices.washingtonpost.com/answer-sheet/higher-education/new-analysis-of-violence-on-ca.html>

(Florida) MacDill's Dale Mabry re-opened after driver attempts illegal entry. Officials at MacDill Air Force Base in Tampa, Florida were forced to close the Dale Mabry gate early Monday because of damage caused by a vehicle trying to make an illegal entry. The gate was re-opened shortly before 10:30 a.m. Security forces at MacDill said they were forced to deploy a emergency mechanism that stops vehicles from entering the base when a car full of people drove past the main gate. Tampa Police say they arrested the people in the car. Security officials at MacDill said there is no reason to suspect terrorism at this point. Before the gate was reopened, motorists had to use the Interbay and Bayshore entrances. Source: <http://www.abcactionnews.com/content/news/local/hillsborough/west/tampa/story/MacDills-Dale-Mabry-re-opened-after-driver/VwmRPDIKiky9o0pYn-jaeg.csp>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

McAfee antivirus program goes berserk, freezes PCs. Computers in companies, hospitals, and schools around the world got stuck repeatedly rebooting themselves on April 21 after an antivirus program identified a normal Windows file as a virus. McAfee Inc. confirmed that a software update it posted at 9 a.m. Eastern time caused its antivirus program for corporate customers to misidentify a harmless file. It has posted a replacement update for download. McAfee could not say how many computers were affected, but judging by online postings, the number was at least in the thousands and possibly in the hundreds of thousands. McAfee said it did not appear that consumer versions of its software caused similar problems. In a statement, the company said it is investigating how the error happened "and will take measures" to prevent it from recurring. The computer problem forced about a third of the hospitals in Rhode Island to postpone elective surgeries and stop treating patients without traumas in emergency rooms, said a spokeswoman for the Lifespan system of

UNCLASSIFIED

UNCLASSIFIED

hospitals. The system includes Rhode Island Hospital, the state's largest, and Newport Hospital. In Kentucky, state police were told to shut down the computers in their patrol cars as technicians tried to fix the problem. The National Science Foundation headquarters in Arlington, Virginia, also lost computer access. Intel Corp. appeared to be among the victims, according to employee posts on Twitter. Intel did not immediately return calls for comment. A systems administrator at Illinois State University in Normal, said that when the first computer started rebooting, it quickly became evident that it was a major problem, affecting dozens of computers at the College of Business alone. Source: http://www.nytimes.com/aponline/2010/04/21/business/AP-US-TEC-McAfee-Antivirus-Flaw.html?_r=1

Drug-dealing spammers hit Gmail accounts. Google is investigating a growing number of reports that hackers are breaking into legitimate G-mail accounts and then using them to send spam messages peddling Canadian pharmaceutical websites that promised to send cheap drugs to U.S. customers. The problem started about a week ago but seems to have escalated recently. "The G-mail team takes security very seriously and is investigating the reports we've seen in our user forums over the past few days," Google said April 20 in an e-mailed statement. "We encourage users who suspect their accounts have been compromised to immediately change their passwords and to follow the advice at the following page: G-mail accounts are often compromised after phishing attempts or via malicious programs, which can seek out and log online credentials from a hacked computer. It is not clear what's behind this wave of G-mail attacks. But in forum posts, G-mail users note that hackers appear to be sending spam via G-mail's mobile interface — which gives mobile-phone users a way to check their G-mail accounts. The G-mail users wondered if there may be a bug in the mobile interface that is allowing criminals to send the spam. Source: http://www.computerworld.com/s/article/9175857/Drug_dealing_spammers_hit_Gmail_accounts

Amazon purges account-hijacking threat. Amazon.com administrators April 20 closed a security vulnerability that made it possible for attackers to steal user log-in credentials for the highly trafficked, e-commerce Website. The XSS, or cross-site scripting, bug on Amazon Wireless allowed attackers to steal the session IDs that are used to grant users access to their accounts after they enter their passwords. It exposed the credentials of customers who clicked on this link while logged in to the main Amazon.com page. It was discovered by a researcher from security-consulting company Avnet. The XSS bug was purged from Amazon about 12 hours after The Register brought it to the attention of the Web site's security team. Source: http://www.theregister.co.uk/2010/04/20/amazon_website_treat/

Security vulnerabilities can be found in 38 percent of network devices. A new report presents real-world results — including common security vulnerabilities and violations — unearthed by Dimension Data during the 235 Technology Lifecycle Management (TLM) Assessments it performed for companies in 2009. The report contains results from assessments performed at small, medium and large organizations from around the world. There were several findings, some of the more significant ones were that more than 38 percent of network devices — such as routers, switches, gateways, etc. — exhibited security vulnerabilities, which may expose organizations to external and internal security attacks. Secondly, there was an average of 40.7 configuration violations per network device — increasing the likelihood of network downtime and exposure to risk. Finally, thirty-five percent of all network devices were found to be beyond end-of-sale (EoS), meaning they will be increasingly unsupportable and exposed to risk as they progress toward last-day-of-support (LDoS). In fact, of

UNCLASSIFIED

UNCLASSIFIED

those devices, more than 50 percent were already beyond end-of-software-maintenance (EoSWM) or LDoS. Source: <http://www.net-security.org/secworld.php?id=9169>

Tool allows cracking of Microsoft Office encryption in minutes. An implementation flaw allows attackers to bypass the encryption mechanism used for Microsoft Office documents. Although this is not news, having been made public in 2005, no (officially acknowledged) attack or tool for exploiting the vulnerability has existed until now. Experts said this probably explains why Microsoft has never fixed the problem with an update for older versions of Office. In a presentation at the recent Black Hat security conference, a French crypto expert emphasised that the situation has now changed. He said his tool can decrypt a document within a few minutes. The expert said he began working on the statistical analysis of the RC4 algorithm used in Office back in 1994. Talking to Heise Security, the expert explained why he has only now published his results: "I was employed by the French military at the time. Everything I did was classified. Now I am free to speak about it." The crypto expert's analysis of RC4-encoded data took advantage of the fact that many implementations of the algorithm are flawed. For RC4 to produce reliable encryption, no key can ever be used more than once. For example, the main reason why the WEP (Wired Equivalent Privacy) encryption used in wireless LANs was cracked so thoroughly was that there weren't enough initialisation vectors (IV) to provide sufficient key variations. Frequently, packets appeared that had been encoded via identical combinations of the same IV and an already static password. Source: <http://www.h-online.com/security/news/item/Tool-for-cracking-Office-encryption-in-minutes-979786.html>

Politically motivated attacks could force enterprises to reshape defenses. An emerging wave of politically motivated cyberattacks is reaching critical mass and threatens to redefine the way enterprises build their defenses, according to an April 20 report. Compiled by a well-known botnet researcher of Damballa, the study offers a comprehensive look at the recent trend toward politically motivated cyberprotests, sometimes called hacktivism. While such organized, mass attacks on specific targets are best known for being carried out against rival governments (think Estonia or Georgia) and large companies (think Project Aurora), the new report showed "cyberprotests" can be carried out against any organization, and for myriad reasons. "These types of attacks focus on all types of topics, and they can be executed by thousands of users or even just a few," the researcher observed. The report offered numerous examples of hacktivism in recent years, including the defacement of hundreds of Dutch Web sites in August 2008 by Islamic protesters over the release of the film Fitna, and last summer's distributed denial-of-service (DDoS) attacks on Iranian government sites by supporters of defeated presidential candidates who claimed voting irregularities. Source: <http://www.darkreading.com/securityservices/security/cybercrime/showArticle.jhtml?articleID=224400721>

Cyberattack on Google said to hit password system. Ever since Google disclosed in January that Internet intruders had stolen information from its computers, the exact nature and extent of the theft has been a closely guarded company secret. But a person with direct knowledge of the investigation now said that the losses included one of Google's crown jewels, a password system that controls access by millions of users worldwide to almost all of the company's Web services, including e-mail and business applications. The program, code named Gaia for the Greek goddess of the earth, was attacked in a lightning raid taking less than two days last December, the person said. Described publicly only once at a technical conference four years ago, the software is intended to enable users and employees to sign in with their password just once to operate a range of services. The intruders

UNCLASSIFIED

UNCLASSIFIED

do not appear to have stolen passwords of G-mail users, and the company quickly started making significant changes to the security of its networks after the intrusions. But the theft leaves open the possibility, however faint, that the intruders may find weaknesses that Google might not even be aware of, independent computer experts said. Source:

<http://www.nytimes.com/2010/04/20/technology/20google.html>

Symantec logs 100 percent rise in new malware. More than 240 million new, malicious programs were discovered last year, with cyber criminals increasingly focusing on Web-based and targeted attacks, according to the latest annual Symantec Internet Security Threat Report. The findings for 2009 showed a 100 percent year-on-year increase in new malware, and a Symantec solutions architect said that one new botnet-infected computer is detected worldwide every 4.6 seconds. The architect warned that malicious activity is taking root especially in developing countries, where less-experienced users are coming online without investing in security tools to protect Internet-connected devices. These countries have also become a source of malicious activity, she added, because many do not have the legislation in place to crack down on cyber crime. Web-based attacks continue to be the most common form of attack, and browser vulnerabilities are increasingly being targeted, the architect explained. The report also highlighted the growing problem of sophisticated attacks targeting specific enterprises, often with the aim of stealing intellectual property rather than customer credit card or bank account details. Source:

<http://www.v3.co.uk/v3/news/2261607/symantec-discovers-100-per-cent>

Mac OS X malware turns into botnet. Security researchers have warned that a rash of malware for Mac OS X systems is now being used to run a botnet. The Trojan malware was first spotted in January, and had been bundled into pirated copies of Mac OS software. Researchers noted at the time that the payload included tools which could allow an attacker to remotely take control of an infected system. It now appears as if those components are being put to use. Symantec researchers said that systems infected by the Trojan have been used in at least one denial-of-service attack. Other users are also reporting that their systems are displaying activity caused by the malware. News of the botnet marks what experts have warned is a small but growing crop of malware targeting OS X systems. Source: <http://www.v3.co.uk/vnunet/news/2240521/mac-malware-turns-botnet>

OWASP issues top 10 web application security risks list. The Open Web Application Security Project (OWASP) Monday issued the final version of its new Top 10 list of application security risks. The list, which was first unveiled in November at the OWASP conference, is a departure from OWASP's previous lists, which ranked the most commonly found weaknesses and vulnerabilities in Web applications. OWASP's new list features the most exploitable and likely security risks found in these apps. OWASP reworked the list to provide developers with more of a reality check and understanding of the real threats, OWASP members said. "This is putting it into perspective ... looking at the things that are most likely to be exploited and how useful [this flaw or weakness] would be for an attacker to get access to an application or sensitive information," said a member of OWASP who worked on the list and who is a security researcher with Rapid7. Source:

http://www.darkreading.com/vulnerability_management/security/app-security/showArticle.jhtml?articleID=224400676

UNCLASSIFIED

NATIONAL MONUMENTS AND ICONS

(Ohio) Man charged in Wayne National Forest blaze. The U.S. Department of Agriculture's Forest Service on Monday charged a man with causing a brush fire that burnt more than 75 acres in a national park in Ohio earlier this month. The man was charged with failing to control a burn on private property, a news release from the forest service said. The 25-year-old suspect was allegedly burning debris when the fire spread to the Wayne National Forest. The fire burned for several hours in the area northwest of Nelsonville, between Door Run Road and U.S. 33. U.S. Route 33 was shut down for a several hours as crews battled the blaze. No homes were damaged and no injuries were reported. If found guilty, the suspect faces a fine of up to \$5,000 and six months in prison. The forestry service said Ohio law prohibits outdoor debris burning from 6 a.m. to 6 p.m. during the months of March, April, May, October and November. Source:

<http://www.10tv.com/live/content/local/stories/2010/04/19/story-nelsonville-brush-fire-man-charged.html?sid=102>

(Kentucky) LBL managers to burn 24,000 acres. Managers at Land Between the Lakes in Golden Pond, Kentucky propose burning almost 24,000 acres of the federal recreation area this year and early next year. The Paducah Sun reported the U.S. Forest Service plan for five prescribed burns on the 170,000-acre reserve would be the most burned in any year. "The prescribed burn is a good tool — you can treat so many acres and it's cost effective," said a LBL forester. "You could do a lot of disturbance with machinery, but it would come with a much bigger price." The controlled fires reduce fuel for wildfires and help the forest grow oak and hickory trees, which are beneficial to wildlife, and take out young shade-tolerant trees like maples. Among new listings is a 7,101-acre burn identified as the Crossroads Prescribed Fire at the northwest tip of LBL. Burns so far this spring have included 3,359 acres in the southern end of LBL near Dover, Tennessee, and one near Wranglers Campground. The area supervisor said the proposed projects and a contact person to receive public comments are listed on the LBL Web site. Source:

<http://www.theleafchronicle.com/article/20100420/NEWS01/4200321/LBL+managers+to+burn+24+000+acres>

POSTAL AND SHIPPING

(Pennsylvania) Bomb squad called to Dauphin County post office. Federal investigators are looking into a suspicious package at a Dauphin County (Pennsylvania) post office. A postal worker discovered it last night at the post office on Crooked Hill Road in Susquehanna Township. Officials did not evacuate the building during the incident, but the state police bomb squad was called in to handle the package. The squad detonated it, and determined that it was not a bomb, but investigators said they still do not know exactly what was inside the package. Source:

<http://www.whptv.com/news/local/story/Bomb-squad-called-to-Dauphin-County-post-office/fVp-pJy-bEepXs9CkxxJ9A.csp>

(Virginia) Post office evacuated in Norfolk due to suspicious package. Authorities evacuated the post office at 2461 E. Little Creek Road in Norfolk, Virginia today after someone found a suspicious package. The city's bomb squad investigated and determined it was harmless, said a Norfolk Fire-

UNCLASSIFIED

Rescue battalion chief. Little Creek Road was closed in both directions during the investigation, but opened shortly after 1 p.m. Source: <http://hamptonroads.com/2010/04/post-office-evacuated-norfolk-due-suspicious-package?cid=ltst>

PUBLIC HEALTH

CDC launches surveillance system to improve blood transfusion safety. A system launched in February by the U.S. Centers for Disease Control and Prevention (CDC) will help track adverse events associated with blood transfusion, according to the Journal of the American Medical Association. An article in the publication said that the system would give hospitals and public health officials tools to help prevent adverse transfusion events. The Hemovigilance Module is the newest component of the CDC's National Healthcare Safety Network, a confidential and voluntary online surveillance system the agency uses to track health-care infections. The module was created by the CDC in collaboration with AABB (formerly the American Association of Blood Banks), an organization that represents institutions and professionals involved in blood transfusion and transplantation. Source: <http://jama.ama-assn.org/cgi/content/extract/303/15/1467>

FDA reviewing use of antibacterial products. The antibacterial chemical found in liquid hand soaps, deodorant bar soaps, toothpastes and more may harm humans and wildlife. Industry groups have said they have provided volumes of information on the benefits and safety of the products. The Food and Drug Administration (FDA) announced April 8 that it will be taking a look at the safety of a widely used antibacterial chemical, triclosan. Triclosan — as well as its cousin triclocarban — is found in liquid hand soaps, deodorant bar soaps, face washes, deodorants, toothpastes, and mouthwashes, as well as in germ-fighting cutting boards and socks. In January, a U.S. Representative (D-Mass.) wrote letters to the FDA and the U.S. Environmental Protection Agency, urging them to review new evidence about the potential harms of triclosan. The Representative has called for banning the chemical in personal-care products, citing concerns that widespread use of triclosan may encourage the spread of antibiotic-resistant bacteria and, as it gets washed down millions of household drains, may harm wildlife. Meanwhile, industry groups such as the Soap and Detergent Assn. and the Personal Care Products Council assert that they have provided volumes of information on the benefits and safety of antimicrobial products. In a consumer fact sheet, the FDA said that, at present, triclosan is not known to be hazardous to humans. Still, the agency first proposed regulating the chemical for consumer use in the 1970s and has revisited the issue several times since. In a letter responding to the Representative, the agency promised to evaluate the new evidence and come to some conclusion by next spring. Source: [http://www.latimes.com/news/science/environment/la-he-closer-2010041920,0,6550138.story?track=rss&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+latimes/news/science/environment+\(L.A.+Times+-+Environment\)&utm_content=Google+Reader](http://www.latimes.com/news/science/environment/la-he-closer-2010041920,0,6550138.story?track=rss&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+latimes/news/science/environment+(L.A.+Times+-+Environment)&utm_content=Google+Reader)

(Tennessee) Two dead in hospital shooting, 2 others injured. The Parkwest Medical Center in Knoxville, Tennessee, will have chaplains and counselors available throughout the day Tuesday after an apparent murder-suicide left one of its employees dead and two wounded. A gunman shot three women outside the hospital Monday afternoon before apparently turning the gun on himself, police said. One of the victims died from gunshot wounds at Parkwest, police said. The suspected gunman also died, said Knoxville's police chief. The killer's identity was withheld pending family notification.

UNCLASSIFIED

UNCLASSIFIED

Parkwest was locked down immediately after the shooting, but was reopened by Monday evening. "The hospital is open; investigation is continuing," the medical center said in a statement. Source: <http://news.blogs.cnn.com/2010/04/20/two-dead-in-hospital-shooting-2-others-injured/?hpt=T2>

Identifying the geography of flu outbreaks. Seasonal flu tends to move in traveling waves, peaking earliest in western states such as Nevada, Utah, and California and working its way east to New England, causing states like Rhode Island, Maine, and New Hampshire to tend to have the latest peak in seasonal flu, according to a report published last week by public health researchers at Tufts University in Boston. The report's findings were based on analysis of older adults' hospitalization records for the 1991 through 2004 flu seasons which were provided by the Centers for Medicare and Medicaid Services, and identified more than 248,000 hospitalization records relating to flu. "Because the peak of seasonal flu runs its course nationwide in a matter of weeks, it is often too late to adjust resources including vaccinations and antivirals once the first outbreak hits. We have identified patterns in seasonal flu and developed a model that allows us to better predict outbreak peak timing," the senior author, a professor of public health and community medicine at Tufts University School of Medicine, said in a statement accompanying the report. Source: <http://www.hstoday.us/content/view/12963/149/>

HHS publishes online list of patient data breaches. The Health and Human Services Department (HHS) has started publishing an online list of more than 60 recent breaches of private, patient health-care data and intends to share the data for research and investigation. Under the economic stimulus law, HHS got authority to publish breach incidents that affect 500 or more persons. Covered entities, including physicians, hospitals and other health-care providers, are required to report breaches of unsecured, protected health information to the department in 60 days. HHS's Office for Civil Rights in recent weeks began publicizing data breaches that affect more than 500 people, dating from July 2009 to March 2010. As of today, the Web site lists 64 breach incidents. The largest breach is that of Blue Cross Blue Shield of Tennessee, where theft of hard drives affected data from more than 500,000 patients in October 2009. Most of the incidents involved theft or unauthorized access to laptop computers or other devices, but some involved hacking and scamming. HHS described how it will share information on the breaches in an April 13 Federal Register notice. Source: <http://fcw.com/articles/2010/04/19/hhs-publishing-online-list-of-patient-data-breaches.aspx>

Microsoft wants pacemaker password tattoos. A Microsoft researcher has suggested tattooing passwords on patients with pacemakers and other implanted, medical devices to ensure the remotely controlled gadgets can be accessed during emergencies. The proposal is the latest to grapple with the security of implanted, medical devices equipped with radio transmitters that can be controlled without the need for surgery. Besides pacemakers, other types of potentially vulnerable devices include insulin pumps and cardiac defibrillators. In 2008, researchers demonstrated that heart monitors were susceptible to wireless hacks that caused pacemakers to shut off or leak personal information. But equally devastating are scenarios where physicians are unable to provide emergency care because they don't have the access codes needed to control the devices. In a paper published last week, the researcher proposed permitting access to such devices to be controlled with encryption similar to what's used on wifi networks. Access keys would then be tattooed on patients using ink that's invisible under most conditions. Source: http://www.theregister.co.uk/2010/04/16/pacemaker_security_tattoo/

UNCLASSIFIED

UNCLASSIFIED

(North Carolina) Hospira says it received 2 FDA warning letters. Hospira Inc. said April 16 it received a warning letter from the Food and Drug Administration after it discovered manufacturing problems at two facilities in North Carolina. The Lake Forest, Illinois company said the FDA sent an April 12 warning letter after inspecting manufacturing facilities in Rocky Mount and Clayton. Hospira said it was informed that emulsion products at the Clayton facility did not meet manufacturing standards, and that manufacturing processes at Rocky Mount were not properly validated. Some problems were repeat violations that were first discovered in an April 2009 inspection. The warning letter does not bar Hospira from making or selling any products, but the company said it will delay shipments of some products until it can investigate and discuss the warnings with the FDA. Hospira said it plans to conduct a comprehensive review of manufacturing operations to make sure they are in compliance with government standards. It also plans to make a full response to the FDA's letter. Source: <http://www.businessweek.com/ap/financialnews/D9F4DS881.htm>

TRANSPORTATION

(Florida) Man drives BMW on runway, parks under jet. According to Lakeland (Florida) Police, one of their officers was working at the Sun and Fun Fly In at Lakeland Linder Regional Airport providing security for the Thunderbird F-16's when he saw a man drive a BMW onto the runway, under a USAF cargo airplane, and in front of a Thunderbird jet. The man was unable to explain how he was able to enter the fenced, secured perimeter of the airport. Each point of entry is clearly posted with a sign that says, "Restricted Area, No Trespassing, Authorized Vehicles Only." The man initially told cops he was a volunteer at Sun and Fun, but couldn't back his story up. The man was placed under arrest for trespass on airport property and transported to Polk County Jail. Source: http://weblogs.sun-sentinel.com/news/specials/weirdflorida/blog/2010/04/man_drives_bmw_on_runway_parks_1.html

Oversight report finds state, traffic-safety data systems improving. A recent government oversight report found the quality of traffic-safety data systems vary by state and while gains are being made, limited resources and coordination can thwart further progress. The U.S. Government Accountability Office analyzed traffic records assessments and found that the quality of state, traffic-safety data systems differed across the six types of data systems maintained by states. Those data systems include vehicle, driver, roadway, crash, citation and adjudication and injury surveillance. Highlights of the report include: Across all states, vehicle and driver data systems met performance measures (which includes timeliness, consistency, completeness, accuracy, accessibility and integration) 71 percent and 60 percent of the time, respectively; while roadway, crash, citation and adjudication, and injury surveillance data systems met performance measures less than half the time. Data system quality varies by performance measure. For example, across all data systems, states met the performance measure for consistency 72 percent of the time, but states met the integration performance measure 13 percent of the time. Of the 51 assessments the GAO reviewed, 49 had insufficient information to fully determine the quality of at least one data system. Furthermore, an updated assessment format has resulted in more frequent instances of insufficient information. Source: <http://www.govtech.com/gt/articles/754502>

WATER AND DAMS

(Indiana) Invasive zebra mussel found in Geist Reservoir. Indiana State wildlife officials said the invasive, zebra mussel has been found in a Central Indiana reservoir that supplies drinking water to

UNCLASSIFIED

UNCLASSIFIED

the Indianapolis area. Last week, a fisherman discovered the mussel in the reservoir that flows from Fishers into the Indianapolis Northeastside, the Indiana Department of Natural Resources (DNR) said Monday. The adult-sized mussel with a brown-and-white shell was found hooked on a Chinese mystery snail, said the aquatic invasive species coordinator with the DNR division of fish and wildlife. He said the effect of zebra mussels can be devastating wherever the invasive species successfully colonizes. Zebra mussels are known for clogging drainage and filtration pipes and can attach to virtually anything in the water column, including rocks, limbs, piers or even boats, he said. The mussels also feed by filtering tiny plants called phytoplankton, which is a major food source for fish and other aquatic life, according to a DNR news release. It said that this marks the first time the species has been found in the Indianapolis area. The zebra mussel has previously been found in more than 65 bodies of water in 44 counties statewide, DNR officials said. Source:

<http://www.indystar.com/article/20100419/LOCAL/100419039/Invasive-zebra-mussel-discovered-in-Geist>

Study: Bacteria highly effective at degrading contaminants. A researcher at Idaho National Laboratory (INL) is conducting studies on the potential of bacteria to treat wastewater, according to nanotech-now.com. An INL environmental microbiologist has found that naturally occurring microbes can be highly effective at degrading contaminants, the article stated. She said that her research could offer a cheaper method for cleaning up underground contaminant plumes. Source:

http://watertechonline.com/news.asp?N_ID=73907

NORTH DAKOTA HOMELAND SECURITY CONTACTS

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **Fusion Center (24/7):** 866-885-8295; email: ndslic@nd.gov ; FAX: 701-328-8175

State Radio: 800-472-2121 **Bureau of Criminal Investigation:** 701-328-5500 **Highway Patrol:** 701-328-2455

US Attorney's Office Intel Analyst: 701-297-7400 **Bismarck FBI:** 701-223-4875 **Fargo FBI:** 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168



UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED